

**DETAILED ACTION**

***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/15/2010 has been entered.

***EXAMINER'S AMENDMENT***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was (tentatively) given in a telephone interview with Mr. Sadr on 11/18/2010.

**Please amend the application as follows:**

Claims 31-32 should be amended to the claim language as shown below.

These amended claims will **replace** claim 31-32 as filed on 10/28/2010:

In claim 31, the amendment filed on 10/28/2010 **has been changed to --**

A non-transitory computer-readable recording medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising:  
dividing content data of a plurality of data files into separate content data portions;

storing the separate content data portions, a block permission table, an integrity check value for the block permission table generated based on a memory unit identifier, and a security header in a memory unit having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of sectors each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity, for each data file of the plurality data files, a first portion is stored in a first sector of one of the plurality of blocks, a second portion is stored in a second sector of one of the plurality of blocks, and a security header corresponding to the content data of the plurality of data files is stored in at least one header block of the plurality of blocks that is different from each one of the blocks in which the content data of the plurality of data files is stored;

encrypting, prior to storing, the content data portions by performing sector level encryption using a first encryption key to execute encryption of each first sector of each of the plurality of blocks, and using a second encryption key that is different from the first encryption key to execute encryption of each second sector of each of the plurality of blocks; and

checking the integrity of the revocation list and the block permission table based on the integrity check value generated based on the memory unit identifier,

wherein the security header stored in the header block includes each encryption key used for each sector of the plurality of blocks.--

In claim 32, the amendment filed on 10/28/2010 **has been changed to --**

A non-transitory computer readable recording medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising:

reading encrypted content data portions, which together comprise encrypted content data of a plurality of data files, a block permission table defining memory-access control information, an integrity check value for the block permission table generated based on a memory identifier, and a security header from a memory having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of sectors each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity, wherein, for each data file of the plurality data files, a first portion is read from a first sector of one of the plurality of blocks, and a second portion is read from a second sector of one of the plurality of blocks, and wherein each first sector of each of the plurality of blocks is encrypted using a first encryption key, and each second sector of each of the plurality of blocks is encrypted using a second encryption key that is different from the first encryption key, and the security header, corresponding to the encrypted content data of the plurality of data files, is read from at least one header block of the plurality of blocks, wherein the at least one header block is different from each one of the blocks in which the content data of the plurality of data files is stored;

decrypting the content data portions stored in each of the sectors by performing sector level decryption by using a first decryption key to decrypt data read from the first sector of each of the plurality of blocks and using a second decryption key that is different from the first decryption key to decrypt data read from the second sector of each of the plurality of blocks; and

checking the integrity of the block permission table based on the integrity check value generated based on the memory identifier,

wherein the security header read from the header block includes each encryption key used to encrypt each encrypted content data portion read from each of the plurality of blocks.--

***Allowable Subject Matter***

Claims 1, 5-6, 8, 12-13, 17, 21-22, 24, 28-29, and 31-32 are allowed.

The following is an examiner's statement of reasons for allowance: The above mentioned claims are allowable over the prior arts because the CPA (Cited Prior Arts) of record taken singly or in combination fail to anticipate or render obvious the specific added limitations, as recited in independent claims 1, 8, 17, 24, 31-32 and subsequent dependent claims.

The CPA does not teach or suggest (in combination with the other claimed limitations) a recording device/method/non-transitory computer recording medium comprising a memory unit for storing a plurality of blocks containing a portion of one of the plurality of data files in a first sector of one of the blocks; a second portion in a second sector of a block; and a cryptosystem unit for performing sector-level encryption where each of the first sectors of each of the plurality of blocks is encrypted using a first key and where each of the second sectors of the plurality of blocks is encrypted with a second key. The CPA further fails to teach/suggest (in combination with the other claimed limitations) wherein the header block includes security header information with the encryption keys and wherein the header block is contained within a different block than each of the blocks containing content data.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

/Nadia Khoshnoodi/  
Examiner, Art Unit 2437  
11/18/2010

NK

/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art Unit 2437